Current Developments of IEEE 1588 (Precision Time Protocol)

Kilian Rösel, Max Helm*, Johannes Zirngibl*, Henning Stubbe*
*Chair of Network Architectures and Services, Department of Informatics
Technical University of Munich, Germany
Email: roeselk@in.tum.de, helm@net.in.tum.de, zirngibl@net.in.tum.de, stubbe@net.in.tum.de

***Abstract*—Precise synchronization of clocks is essential for multiple scientific and industrial applications. Synchronization in networks can be achieved with the IEEE 1588 Precision Time Protocol. This paper gives an overview of this protocol and explores recent developments of this standard. It examines new features for accuracy and security introduced by the 2020 released IEEE 1588-2019 (PTPv2.1) edition of this protocol. Sub-nanosecond accuracy gets supported by the High Accuracy Profile based on the White Rabbit Extension, utilizing Layer 1 signals and a system wide calibration procedure. Several approaches to make the synchronization mechanism more secure are presented. Finally the paper outlines the expected impact of PTPv2.1 functionality on industrial use cases.**

***Index Terms*—IEEE 1588, precision time protocol, high accuracy**

1. Introduction

Precise synchronization of clocks in distributed systems is a major requirement in several areas such as telecommunication, finance and power grid. However, many solutions lack in synchronization accuracy, robustness and security to be properly deployed in real industrial scenarios [1].

On 16 June 2020 the IEEE 1588-2019 [2] version of the Precision Time Protocol (PTP) superseded the previous IEEE 1588-2008 (PTPv2) [3] version. This new revision includes the High Accuracy Profile (HA), which allows to achieve sub-nanosecond accuracy as well as several mechanisms to make PTP systems more secure and robust.

This paper gives an overview over the PTP protocol in Section 2. The different PTP devices with their topology and the synchronization mechanism will be discussed. The new High Accuracy Profile allows to achieve sub-nanosecond accuracy. It relies on two key mechanisms: Firstly, calibration and measurement of asymmetries and secondly achieving higher precision in timestamping, presented in Section 3. Furthermore, new features and guidelines for security are presented in Section 4. This paper finally discusses new possibilities and challenges of PTPv2.1 in PTP implementations based on different industries in Section 5.

2. Background

A PTP network consists of multiple PTP devices and non-PTP devices, such as switches and routers.

An Ordinary Clock (OC) is a terminal device which has only one PTP port and maintains the timescale with its local clock. It can either be the Grandmaster Clock, such that it acts as the source of time or a slave receiving time. When it is in the master state, it often uses global navigation satellite systems (GNSS) or terrestrial radio links as time reference.

Boundary Clocks (BC) are network devices with multiple PTP ports. One of them is in the SLAVE state, so they can synchronize their own local clock to the time source. The ports in the MASTER state provide time to other PTP Instances.

End-to-end (E2E) and peer-to-peer (P2P) Transparent Clocks (TC) are network devices as well, but do not synchronize their own internal clock. Instead they measure the residence time of PTP messages and propagate them after adjusting a correction field.

Management Nodes are devices used for configuring and monitoring clocks in a PTP network.

Non-PTP devices such as switches and routers, can cause inaccuracies because they introduce asymmetry in the network through queueing effects. For achieving high accuracy it is therefore essential to only use BCs and/or TCs as network devices.

The logical unit in which the PTP devices synchronize to one timescale is called a domain. Originally multiple domains could exist in the same network, but were strictly separated. The new edition introduces the possibility of inter-domain interactions between PTP devices. This feature can get used to enhance security, presented in Section 4.

2.1. Master-Slave Hierarchy

The PTP domain has to be organized in a treelike master-slave hierarchy, with the best suited clock as grandmaster at the root. To select the grandmaster and to negotiate this topology the Best Master Clock Algorithm (BMCA) may be used. First OCs and BCs exchange the following performance properties via *Announce* messages:

1) priority1: Can be set by administrators to apprise their preferred master clock.
2) clockClass: Describes the traceability, synchronization state and expected performance.
3) clockAccuracy: Describes the accuracy of the Local PTP Clock.
4) offsetScaledLogVariance: Describes the stability of the Local PTP Clock.
5) priority2: Can be set by administrators to arrange equivalent PTP Instances.

doi: 10.2313/NET-2021-05-1_04

6) clockIdentity: Unique identifier for PTP Instances to break ties.

Secondly, each PTP Instance computes the states of its ports according to those properties.

The BMCA also prunes mesh topologies to avoid cyclic network connections. It does so by setting ports on PASSIVE state such that there is no time synchronization on this connection. This way endless circulation of rogue *Announce* messages can be avoided. Figure 1 shows an exemplary PTP network with pruned mesh topolgy [2].

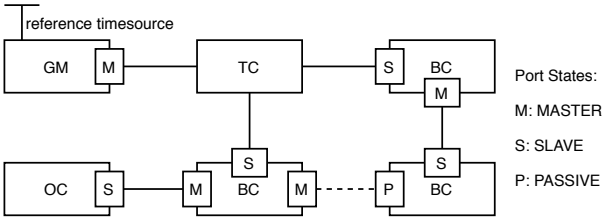

Figure 1: Example PTP network with pruned mesh topology [2].

The BMCA is running continuously, even when the desired topology is already established. This way the network can reconfigure itself automatically, if for example physical connections get lost or the performance properties of a Grandmaster Clock degrade [2].

The new edition of the standard also includes mechanisms for manual configuration of PTP port states. However, setting port states manually may result in "timing islands" where time does not get distributed, illustrated in Figure 2. Additionally it disables automatic reconfiguration [4].

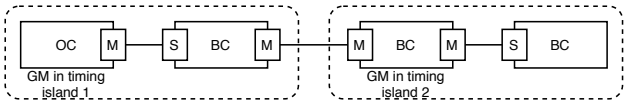

Figure 2: Adjacent ports in master state result in timing islands [4].

2.2. Synchronizing Mechanisms

The time synchronization mechanism takes place between two linked Ordinary and/or Boundary Clocks. One of them is in the master state, the other one in the slave state. They are exchanging a series of event and general messages to calculate the offset of the Slave Clock with respect to the master clock. Event messages are messages that get timestamped when they egress or ingress a port. General messages are not required to be timestamped. Details on timestamp generation are shown in Section 2.3. Eventually, all PTP Instances are synchronized to the grandmaster as time gets distributed through the hierarchy.

To distribute time, the master clock first sends a *Sync* message to the Slave and timestamps the departure time t_1. The slave timestamps the arrival of this message t_2. In a two-step setup the master then sends a *Follow_Up* message containing t_1. In a one-step setup the master clock would already have included timestamp t_1 in the first *Sync* message, rendering the *Follow_Up* message obsolete. In order to calculate the network delay according to the E2E mechansim the Slave clock then sends a *Delay_Req* message, and notes the departure time t_3. The master creates timestamp t_4 at arrival of this message and communicates this timestamp via a *Delay_Resp* to the slave. Figure 4 illustrates this message exchange. When the slave clock possesses all four timestamps, it can compute the mean path delay d and its offset to the master o:

$$d = \frac{(t_2 - t_1) + (t_4 - t_3)}{2}$$
$$o = (t_2 - t_1) - d$$

Knowing the slave-master offset the slave clock can adjust its own clock and is then synchronized to the master.

Calculation of the network delay can also be done with the P2P mechansim. This mechanism does not calculate the network delay between a master and slave port, but between directly neighbouring nodes. The P2P network delay then gets added up along the whole path. Figure 3 illustrates the difference between P2P and E2E.

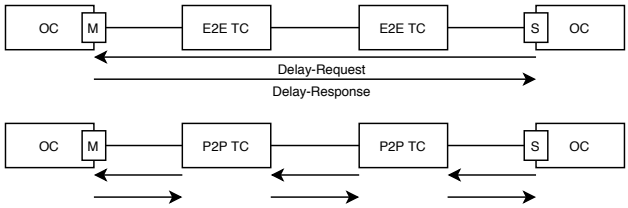

Figure 3: PTP Delay Mechanism [5]

This model assumes the master-slave (t_{ms}) and slave-master (t_{sm}) propagation delay to be symmetric, i.e. messages need the same time to travel in either direction. However, to achieve high accuracy in real scenarios one must take steps to account for asymmetries in the network. The HA therefore defines a system wide calibration procedure, shown in Section 3.1.

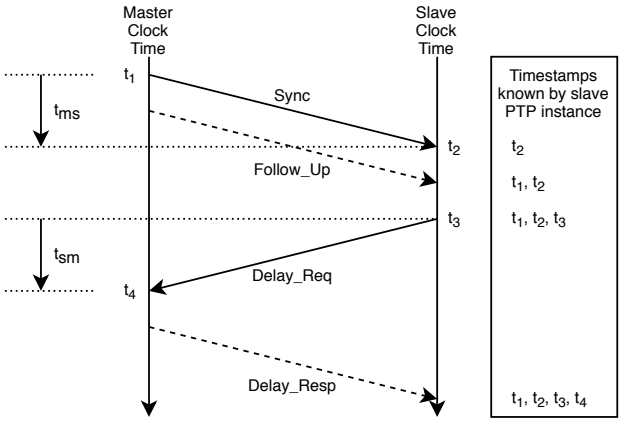

Figure 4: Basic end-to-end PTP Timing Message Exchange [2]

doi: 10.2313/NET-2021-05-1_04

2.3. Timestamp Generation

Precise timestamp generation is crucial for the accuracy of round trip time measurement. A timestamp is defined as the instance the message timestamp point of an event message crosses the reference plane between medium and PTP port. Though in implementations timestamping might take place in the Application Layer (C), in the kernel interrupt service routines (B) or in the physical layer (A), illustrated in Figure 5. Traveling through the protocol stack can introduce latencies, thus it is preferable to choose a point near to the physical layer. In this case, specialized hardware assists in the generation of the timestamp. Nevertheless, any offset from the reference plane has to be compensated for by measurement and calibration [2].

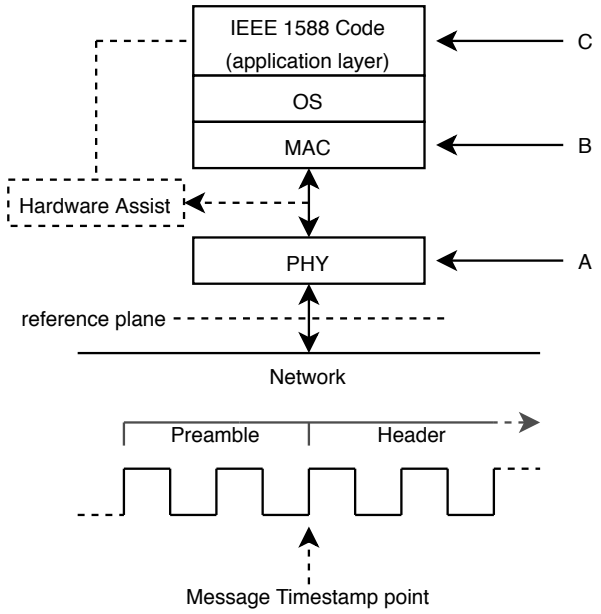

Figure 5: Protocol Stack and Message Timestamp Point [2]

3. High Accuracy

The High-Accuracy Profile is based on the White Rabbit Extension (WR) for PTPv2. WR was developed to renovate the control and timing system at CERN [6] and was later generalized and included in the standard by the P1588 working group [7].

It allows to achieve sub-nanosecond synchronization accuracy by relying on two mechanisms and methodologies: (1) Various sources of asymmetry get recognized, measured and calibrated to compensate for their effects, described in Section 3.1. (2) Utilizing physical transmission and receive signals to increase precision in the hardware assisted timestamping process of PTP event messages, described in Section 3.2 [8].

3.1. Calibration

Asymmetries between two PTP Instances introduce inaccuracy in the synchronization process. There are two sources of asymmetry: timestamp generation latencies and medium asymmetry. Knowing the values allows to compensate for their effects when calculating the offset from the master.

Timestamp generation latencies get introduced on egress and ingress of messages, e.g. because timestamps are captured at a point removed from the reference plane, see Section 2.3. Medium asymmetries originate from the physical communication medium. They can for example be caused by the use of different wavelengths of light in single-strand fibers. The standard defines several procedures, how to calibrate these latencies and asymmetries. Because of different optical phenomena in long distance optical links, these procedures are only intended for Local Area Networks [2]. However, deployment of long distance fiber links has already been investigated [9].

3.2. Precise Timestamping

The accuracy of delay measurements relies on the resolution and precision of timestamping. Timestamps are created by the Local PTP Clock whenever the message timestamp point crosses the implemented point in the protocol stack, see Section 2.3. However, usually the receive and transmit signals on the Physical Layer (L1) are different from the Local PTP Clock signal used for timestamping. This may result in timestamping imprecision. For example, a Local PTP Clock with a frequency of 125 MHz is limited to a resolution of 8 ns [8].

To correct for this imprecision, knowledge about the phase offset between the L1 transmit clock signal (clk_{txL1}), L1 receive clock signal (clk_{rxL1}), and the Local PTP Clock ($clk_{localPTP}$) is required. The L1 tx/rx signals are the physical signals used by the medium to transport signals over the wire. The reception phase offset (x_{rx}) and transmission phase offset (x_{tx}) is the offset between the Local PTP Clock signal to the L1 receive signal and L1 transmission signal respectively. This relationship gets demonstrated in Figure 6. Note that the transmit signal of Clock A is the receive signal of Clock B. Knowing the value of x_{rx} and x_{tx} at the instance of the timestamp allows then to compensate the offsets in the calculation process.

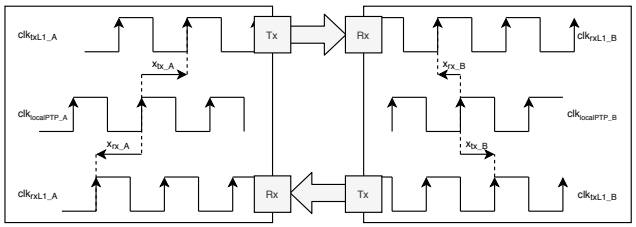

Figure 6: Link Reference Model between two Clocks [8]

Quantifying the phase offsets depends on the variability of the offset. In the simplest case the offsets are constant. That means the L1 tx/rx signals and the Local PTP clock signal are coherent, i.e., they operate on the same frequency. To achieve coherency, ports can base their Local PTP Clock signal on the L1 rx signal recovered from the medium and generate their L1 tx signal from the Local PTP Clock. With this relationship in place, the

doi: 10.2313/NET-2021-05-1_04

constant offsets can be measured, for example by using Digital Dual Mixer Time Difference (DDMTD) phase detection [10].

Syntonization in networks can for example be achieved with Synchronous Ethernet (ITU-T Recommendations G.8261 [11] and G.8262 [12]). The PTP Clocks can then take advantage of the Layer 1 syntonization to enhance their timestamping precision [8].

4. Security Mechanisms

Security concerns have long been neglected in the development of PTP. Especially in critical infrastructures such as the power grid this might prove fatal. However, PTPv2.1 describes several mechanisms to make PTP more secure [13].

PTP Integrated Security Mechanism. PTP messages can be extended by a type, length, value (TLV) extension mechanism in order to transfer additional information. There are several different types of TLVs defined.

The AUTHENTICATION TLV, providing a way to authenticate PTP messages, was already introduced in PTPv2. But test implementations of this feature have shown little additional security at the expense of overhead [14]. PTPv2.1 revised the AUTHENTICATION TLV feature.

The included integrity check value (ICV) verifies all fields from the PTP Header up to the AUTHENTICATION TLV without including the ICV itself. Also included in the calculation is a secret key. This key has to be distributed by a key management system. Depending on this system two different verification schemes are possible: (1) Immediate security processing enables verification of the message immediately. To achieve this, the secret key has to be known to the communication partners before processing. This approach also allows mutable fields. For example a transparent clock can adjust the correction field and can then recompute the ICV. (2) Delayed processing enables to share the secret key after message transmission. With this approach the receiver has to store the message until he receives the key to verify it. Those two approaches can also be combined. Figure 7 shows this case. Everything after the first AUTHENTICATION TLV is immediately verified. This method allows to add TLVs that can be modified by intermediate devices [13].

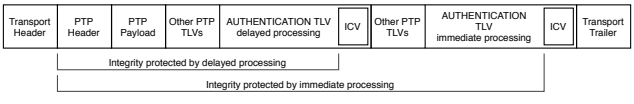

Figure 7: Authentication TLV [2]

The key management system is responsible for the distribution of keys, however the standard does not yet define such a system, but merely gives guidelines [15].

PTP External Transport Security Mechanisms. The standard suggests using MACSec and IPSec as external security mechanisms. Those protocols provide protection against several attacks, as shown by [16].

Architecture Mechanisms. The standard presents various guidelines to enhance security by architectural choices based on redundancy: (1) Redundancy by complementary timing systems means that end-users of time obtain a second reference through a non-PTP way, for example by GPS. This way they can detect malicious behaviour. (2) Multiple domains with separate Grandmaster Clocks work together through inter-domain interactions. End users then can obtain time in a voting process from multiple domains and are therefore able to exclude malfunctioning time information. (3) Lastly redundant network paths between nodes can ensure distribution of timing messages even when some connections get lost [2].

Monitoring and Management Mechanisms. Monitoring and managing the performance of the PTP network can reveal clues about potential security attacks, e.g. delay attacks. These can be identified by detecting unexpected offset jumps or large changes in measured path delays. The new version has also introduced a standardized format in which all PTP devices can share their performance data in an uniform way with Management Nodes [2].

5. Applications of PTPv2.1 Functionality

The White Rabbit Extension has already proven useful in multiple scientific applications, e.g. in particle accelerators. But also other sectors have already made endeavours in adapting this technology [17]. Deutsche Börse, for example, uses WR to synchronize their own timestamping devices. Additionally they provide means for their trading partners to synchronize their own clocks to theirs [18]. As the WR technology matures through the standardization as High Accuracy Profile, it will grow even more attractive for industrial use. So it is to be expected to see an adaption in multiple areas. Especially the operation of power grids can profit from increased timing accuracy. As the grid evolves to being powered by sustainable but unpredictable energy sources, precise monitoring is essential. For example, multiple synchrophasers can detect characteristic voltage spikes caused by malfunctioning equipment. When the measurements are precisely synchronized conclusions on the origin can be drawn [19].

Deployment in such critical infrastructure was previously hampered by security concerns. An implementation of the AUTHENTICATION TLV feature for Linux PTP has already proven to be feasible with a low computational overhead [13]. This result and the other security guidelines may encourage adopters in utilizing PTPv2.1 functionality in their own implementations.

6. Conclusion and Future Work

The new version includes options for achieving high accuracy and mitigating security risks. These two features are essential for PTP to be further adapted as time synchronization technology. This paper has presented these new features and has briefly outlined their impact on industrial scenarios. However, PTPv2.1 includes even more innovations, not presented in this paper, such as profile isolation, special PTP ports and mixed multicast/unicast operation [20].

doi: 10.2313/NET-2021-05-1_04

References

[1] F. Girela-López, J. López-Jiménez, M. Jiménez-López, R. Rodríguez, E. Ros, and J. Díaz, "IEEE 1588 High Accuracy Default Profile: Applications and Challenges," *IEEE Access*, vol. 8, pp. 45 211–45 220, 2020.

[2] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," *IEEE Std 1588-2019 (Revision of IEEE Std 1588-2008)*, pp. 1–499, 2020.

[3] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," *IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002)*, pp. 1–300, 2008.

[4] D. Arnold, "What's in IEEE 1588-2019: DIY PTP Port States," https://blog.meinbergglobal.com/2020/07/24/whats-in-ieee-1588-2019-diy-ptp-port-states/, 2020, [Online; accessed 24-September-2020].

[5] Z. Idrees, J. Granados, Y. Sun, S. Latif, L. Gong, Z. Zou, and L. Zheng, "IEEE 1588 for Clock Synchronization in Industrial IoT and Related Applications: A Review on Contributing Technologies, Protocols and Enhancement Methodologies," *IEEE Access*, vol. 8, pp. 155 660–155 678, 2020.

[6] "The White Rabbit Project," https://white-rabbit.web.cern.ch/Default.htm, 2020, [Online; accessed 26-September-2020].

[7] "IEEE P1588 Working Group," https://sagroups.ieee.org/1588/, 2020, [Online; accessed 26-September-2020].

[8] O. Ronen and M. Lipinski, "Enhanced Synchronization Accuracy in IEEE1588," *2015 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, pp. 76–81, 2015.

[9] E. F. Dierikx, A. E. Wallin, T. Fordell, J. Myyry, P. Koponen, M. Merimaa, T. J. Pinkert, J. C. J. Koelemeij, H. Z. Peek, and R. Smets, "White Rabbit Precision Time Protocol on Long Distance Fiber Links," *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control*, vol. 63, no. 7, pp. 945–952, 2016.

[10] P. Moreira, P. Alvarez, J. Serrano, I. Darwezeh, and T. Wlostowski, "Digital Dual Mixer Time Difference for Sub-Nanosecond Time Synchronization in Ethernet," pp. 449–453, 2010.

[11] "Timing and Synchronization Aspects in Packet Networks," *ITU-T G.8261/Y.1361*, pp. 1–120, 2019.

[12] "Timing Characteristics of Synchronous Equipment Slave Clock," *ITU-T G.8262/Y.1361*, pp. 1–44, 2018.

[13] E. Shereen, F. Bitard, G. Dán, T. Sel, and S. Fries, "Next Steps in Security for Time Synchronization: Experiences from implementing IEEE 1588 v2.1," *2019 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, pp. 1–6, 2019.

[14] C. Önal and H. Kirrmann, "Security Improvements for IEEE 1588 Annex K: Implementation and Comparison of Authentication Codes," pp. 1–6, 2012.

[15] D. Arnold, "The PTP AUTHENTICATION TLV," https://blog.meinbergglobal.com/2020/06/04/the-ptp-authentication-tlv/, 2020, [Online; accessed 29-September-2020].

[16] T. Mizrahi, "Time Synchronization Security Using IPsec and MACsec," *2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, pp. 38–43, 2011.

[17] M. Lipiński, E. van der Bij, J. Serrano, T. Włostowski, G. Daniluk, A. Wujek, M. Rizzi, and D. Lampridis, "White rabbit applications and enhancements," *2018 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, pp. 1–7, 2018.

[18] "High Precision Time (White Rabbit) Pilot," https://www.eurexchange.com/ex-en/find/initiatives/technical-changes/high-precision-time-white-rabbit-pilot, 2019, [Online; accessed 3-October-2020].

[19] A. Jarc, "Use Cases for Timing in Power Grids," https://blog.meinbergglobal.com/2019/07/16/use-cases-for-timing-in-power-grids/, 2019, [Online; accessed 3-October-2020].

[20] D. Arnold, "What's In the 2019 Edition of IEEE 1588?" https://blog.meinbergglobal.com/2017/09/24/whats-coming-next-edition-ieee-1588/, 2017, [Online; accessed 3-October-2020].